Syllabus(2026-1st semester)

Course	Digital Forensics	Department	Cyber Security	Office Hours	매주 월요일 14:00 ~ 16:00
Course No. and Class	38497-01	Hours	3.0	Academic Credit	3.0
Professor	Jongkil Kim		Office	Jinseonmi-gwan 225	
Telephone	4253		E-MAIL		
Value of competence	Pursuit of Knowledge(80), Creative Convergence(20)		Keyword	Digital Evidence, Forensic science, Cyber crime	

1. Course Description

This subject is designed to introduce the fundamentals of digital forensics and incident response processes. The content of the subject will include various technical and operational cybersecurity topics related to digital forensics and incident response.

2. Prerequisites

There are no prerequisites for this subject. However, students may need some basic knowledge of cybersecurity.

3. Course Format

Lecture	Discussion/Presentation	Experiment/Practicum	Field Study	Other
80%	0%	20%	0%	0%

- explanation of course format :

The subject will include some hands-on practice (about 20%) together with theoretical lectures (about 80%).

4. Course Objectives

By successfully completing this subject, the students can get solid understanding of digital forensics and incident response processes. Those processes will be explained based on both technical and operational practices such as collecting evidence, analyzing it, and writing incident response reports to prevent further attacks. Therefore, this subject will help students comprehend the roles of digital forensic professionals and enable them to discuss cybersecurity topics with other cybersecurity professionals.

5. AI Use Principles and Guidelines

＊The following items present example principles and guidelines regarding the use of AI in a course. The course professor may revise and supplement them as necessary, depending on the characteristics and needs of the course.

1) General Principles for AI Use

- This course is conducted on the premise of learners'responsible use of AI and academic integrity. Learners are expected to understand and comply with the AI Ethics Guidelines for Learners posted on the THE BEST Integrated Educational Support Service website.
  https://cyber.ewha.ac.kr/ethicsguide.php
- Learners must adhere to the scope of permitted AI use and prohibited practices as specified by the course professor according to the purpose of each assignment, assessment, or learning activity. AI may be used only within the permitted scope.
- When learners use AI to complete assignments, they must clearly disclose the use of AI and submit a Disclosure Statement.

※ The Disclosure Statement includes information such as the purpose of AI use, the stage(s) at which AI was used, the content generated or assisted by AI, and the extent of AI's contribution to the final output.
Examples of Disclosure Statements are available on the THE BEST Integrated Educational Support Service website.

2) Examples of Permitted AI Use

- Information and resource search
- Idea brainstorming
- Improvement of grammar, writing style, and translation
- Data analysis
- Coding and debugging support
- Others ( )

3) Examples of Prohibited AI Use

- Submitting, in whole or in part, AI-generated content as learning outputs (e.g., reports, essays, presentation materials) without the learner’s own revision or supplementation
- Using AI during examinations, quizzes, or other assessments without the course professor's prior permission
- Submitting AI-generated fabricated citations, references, or sources as if they were authentic materials
- Others ( )

4) Consequences for Misuse

- Violations of the AI use policy may be regarded as academic misconduct.
- In the event of academic misconduct, the course professor will determine appropriate follow-up actions after a comprehensive review of the student's explanation, AI usage records, and the writing or development process.

6. Evaluation System

* Absolute evaluation

Midterm Exam	Final Exam	Quizzes	Presentation	Projects	Assignments	Participation	Other
30%	40%	0%	0%	0%	20%	10%	0%

* Evaluation of group projects may include peer evaluations.

- explanation of evaluation system

Grades will be given based on the performances of the exams, assignments, and participation.

7. Required Materials

Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats,

7. Required Materials

2nd Edition
by Gerard Johansen

8. Supplementary Materials

Cybersecurity – Attack and Defense Strategies - Second Edition
By Yuri Diogenes , Dr. Erdal Ozkaya

9. Optional Additional Readings

10. Course contents

Week	Date	Topics, Materials, Assignments
Week 1	2026/03/04(WED)	Introduction of the subject
	2026/03/06(FRI)	Understanding Incident Response
Week 2	2026/03/11(WED)	Understanding Incident Response
	2026/03/13(FRI)	Managing Cyber Incidents
Week 3	2026/03/18(WED)	Managing Cyber Incidents
	2026/03/20(FRI)	Fundamentals of Digital Forensics
Week 4	2026/03/25(WED)	Fundamentals of Digital Forensics
	2026/03/27(FRI)	Collecting Network Evidence
Week 5	2026/04/01(WED)	Collecting Network Evidence
	2026/04/03(FRI)	Acquiring Host-Based Evidence
Week 6	2026/04/08(WED)	Acquiring Host-Based Evidence
	2026/04/10(FRI)	Forensic Imaging
Week 7	2026/04/15(WED)	Forensic Imaging
	2026/04/17(FRI)	Analyzing Network Evidence
Week 8	2026/04/22(WED)	Insider Threat (University Exam Period - The lecture will be provided online via Cybercampus)
	2026/04/24(FRI)	Leveraging Threat Intelligence I (The lecture will be provided online via Cybercampus)
Week 9	2026/04/29(WED)	Midterm Exam
	2026/05/01(FRI)	Labor day
Week 10	2026/05/06(WED)	Analyzing Network Evidence
	2026/05/08(FRI)	Analyzing System Memory
Week 11	2026/05/13(WED)	Analyzing System Memory
	2026/05/15(FRI)	Analyzing System Storage
Week 12	2026/05/20(WED)	Analyzing System Storage
	2026/05/22(FRI)	Analyzing Log Files
Week 13	2026/05/27(WED)	Analyzing Log Files
	2026/05/29(FRI)	Ewha's 140th Anniversary Ceremony
Week 14	2026/06/03(WED)	The 9th Nationwide Local Elections Day
	2026/06/05(FRI)	Malware analysis
Week 15	2026/06/10(WED)	Malware analysis
	2026/06/12(FRI)	Final Exam
Makeup Classes 1	2026/05/01(FRI)	Leveraging Threat Intelligence II (The lecture will be provided online via Cybercampus)

10. Course contents

Week	Date	Topics, Materials, Assignments
Makeup Classes 2	2026/05/29(FRI)	Writing the Incident Report
Makeup Classes 3	2026/06/03(WED)	Writing the Incident Report

11. Course Policies

* For laboratory courses, all students are required to complete lab safety training.

12. Special Accommodations

* According to the University regulation #57, students with disabilities can request special accommodation related to attendance, lectures, assignments, and/or tests by contacting the course professor at the beginning of semester. Based on the nature of the students' requests, students can receive support for such accommodations from the course professor and/or from the Support Center for Students with Disabilities (SCSD).

* The contents of this syllabus are not final—they may be updated.